Oct. 19, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission 445 12th St. SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On Monday, October 17, 2017 Brandi Collins and Anika Collier Navaroli of Color Of Change (COC) met with Claude Aiken, legal advisor to Commission Clyburn to discuss matters in the above referenced proceeding. During the meeting COC shared views on several aspects of the rulemaking and the Chairman's recent fact sheet including pay-for-privacy models, de-identification of data, and the categorization of data as sensitive or non-sensitive.

1. Pay-for-privacy

COC remains firmly against any method that requires payment for data to be protected and any system of payment that would create a two-tiered level of privacy based upon those who can afford to pay and leave behind those who cannot.

While we commend the Commissioner's fact sheet for prohibiting "take-it-or-leave-it" offers, we are concerned with the opt-in allowance made for financial incentive schemes even with the requirement of heightened disclosure and recommend the FCC outright prohibits these schemes as well. With the median income of Black households

in 2015 being $36,898,[1] consent conditioned on an unaffordable premium is not consent at all. And for those individuals with little to no discretionary income, these schemes can be unreasonable no matter the cost.

If the FCC does choose to move forward without outright prohibition of financial incentive schemes, COC urges the Commissioners to ensure that these plans have a clearly articulated and accessible process in which they can be challenged.

2. De-identified Data

COC categorically disagrees with the statement in the fact sheet of the Chairman's proposal that de-identified data "can present fewer privacy concerns than other types of consumer data."[2] By the nature of the Black American experience, individuals belonging to that class tend to have extensive amounts of identifying data publicly available. This sheer volume of data creates even larger public databases from which seemingly anonymized data can be re-identified.

Thus, the privacy concerns as they relate to de-identified data are not lessened as they relate to Black people and communities of color. And we recommend that the carve out for de-identified data not be made by the FCC as we worry that this exception will act as a loophole for BIAS providers to collect, store, and sell data that is purged of data points typically considered to be personally identifying, but with the data largely left intact. This pseudonymized data often can easily be re-identified. To illustrate, computer science professor Latanya Sweeney conducted a study using census data, and found that she could identify 87% of the United States population using simply zip code, birth date, and gender.[3]

In additional to the vulnerability of re-identifying specific individuals, COC also cautions against de-identified data being used to create a model of a larger group of alike individuals. Data points do not exist or operate in a vacuum, the speed and resources made available by very nature of broadband mean that one point is no longer used by

---

[1] Proctor, Bernadette D. and DeNavas-Walt, Carmen, *Income and Poverty in the United States: 2015*,

[2] FCC, Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice over Their Personal Information (Oct. 6, 2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/DOC-341633A1.pdf.

[3] Latanya Sweeney, k-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5), 2002; 557-570.

itself. Marketing and advertising schemes exist to target specific demographics based on assumptions made and collected about a larger group. In the digital context, the amount of de-identified data available to BIAS providers allows them to create models that lay the groundwork for predatory advertising and marketing by third parties.

If the FCC does move forward giving de-identified information a lower level of privacy protection, COC argues that it must lay out a method of oversight and independent verification of the de-identification techniques BIAS providers use. This additional level of scrutiny by the public will help see that consumer information is properly de-identified and the risk of re-identification is lessened.

3. Sensitive and Non-sensitive Data Distinction

COC reiterates our argument that the FCC should not distinguish between sensitive and non-sensitive information and that opt-in consent should be standard for all data. Here, the distinction between what is considered sensitive data and what is considered non-sensitive data is mostly left up to context. Information that for one group is considered innocuous can be considered sensitive to another group, particularly Black people and communities of color.

As COC previously explained,

> non-sensitive information can often be proxy for protected class information in our increasingly data centric world. Using the example of car insurance discounts, COC illustrated how Auto Insurance Telematics Devices collect what would be considered "non-sensitive" data- such as vehicle speed, the time of day someone is driving, the miles driven, and the rates of acceleration and braking. These devices do not collect "sensitive" data- such as location or the driver's identity.[4] By measuring non-sensitive data like the time of day a person is driving, car insurance companies can be engaged in pricing discrimination against individuals who work night shifts and tend to be of lower socioeconomic status and members of communities of color.[5] Thus, regardless of the distinction, information drawn from the non-sensitive data can easily become proxy for

---

[4] Peppet, Scott R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent* (March 1, 2014). Texas Law Review, Forthcoming. Available at SSRN:http://ssrn.com/abstract=2409074

[5] Saenz, Rogelio, *A Demographic Profile of U.S. Workers Around the Clock*, accessed online at http://www.prb.org/Publications/Articles/2008/workingaroundtheclock.aspx, on Sept. 29, 2016.

protected class and sensitive information and we argue that the FCC should not continue to make this distinction. [6]

If the FCC does decide to adopt a framework that relies on this distinction, COC first argues that the framework should be switched to a sensitive-by-default approach. Here, all data and information would automatically be labeled as sensitive and the FCC would then specify which specific information and data should be carved out as non-sensitive. This formulation alleviates the risk to consumers by forcing broadband providers to demonstrate which categories of data are non-sensitive.[7]

Second, if the FCC does not reverse the current framework, COC urges that the FCC must expand the current categories of sensitive information as laid out in the fact sheet to the Commissioner's proposal. Specifically, the framework should include IP address and MAC address, as well as race and gender.

While an IP address on its face can seem innocuous, the information it reveals is very personal in nature. So much so, that the European Union has ruled that they be classified as personal information.[8] IP addresses can often be used to determine the location an internet user lives which in turn can correlate to race and income level.[9] In fact, location and zip code information has been used by Staples and other corporations to institute digital redlining and charge customers of color higher prices for products based solely on their geography.[10] Including IP address in the categories of sensitive information would help ensure this method of digital discrimination and predatory pricing is curtailed.

MAC addresses also provide a view into the protected class and private information of Internet users. Because MAC addresses are assigned to device manufacturers, an individual MAC address can convey what company manufactured a certain device. In the case of technological devices, Black people, communities of color, and low-income

---

[6] Color Of Change Notice of Ex Parte, WC Docket No. 16-106 (Oct. 3, 2016), at 2.
[7] New America's Open Technology Institute Notice of Ex Parte, WC Docket No. 16-106 (Oct. 13, 2016), at 3.
[8] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland (2016) accessed online at http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN&cid=1095511.
[9] Alethea Lange & Rena Coen, *How Does the Internet Know Your Race?*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 7, 2016), https://cdt.org/blog/how-does-the-internet-know-your-race/.
[10] Valentino-Devries, Jennifer, Singer-Vine, Jeremy, and Solanti, Ashkan. "Websites Vary Prices, Deals Based on Users' Information." The Wall Street Journal, December 24, 2012.

individuals over index on Android devices.[11] Thus, access to the MAC addresses of Internet users allows for broadband companies, and the third parties who access this data, to build a profile of that user and their larger demographic which includes protected class information that can and will be used for discriminatory purposes.

COC also argues that race and gender information be included in the category of sensitive information because they are categories of protected class information and should specifically be named as sensitive data to not be collected by BIAS providers.

Respectfully submitted,

Brandi Collins
Director of Campaigns: Economic, Environmental & Media Justice Departments
1714 Franklin Street, #100-136
Oakland, CA 94612
510-663-4840 Ext 19

[11] Edwards, Jim. "These Maps Show That Android Is For People With Less Money." Business Insider, April 3, 2014.